JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY
1990

CROND
CYBER RANGE ORGANIZATION aND DESIGN

Large-scale Testbed and Cyber Range Organization and Design

大規模なテストベッドとサイバーレンジ構成学

Razvan Beuran, Ken-ichi Chinen

Outline

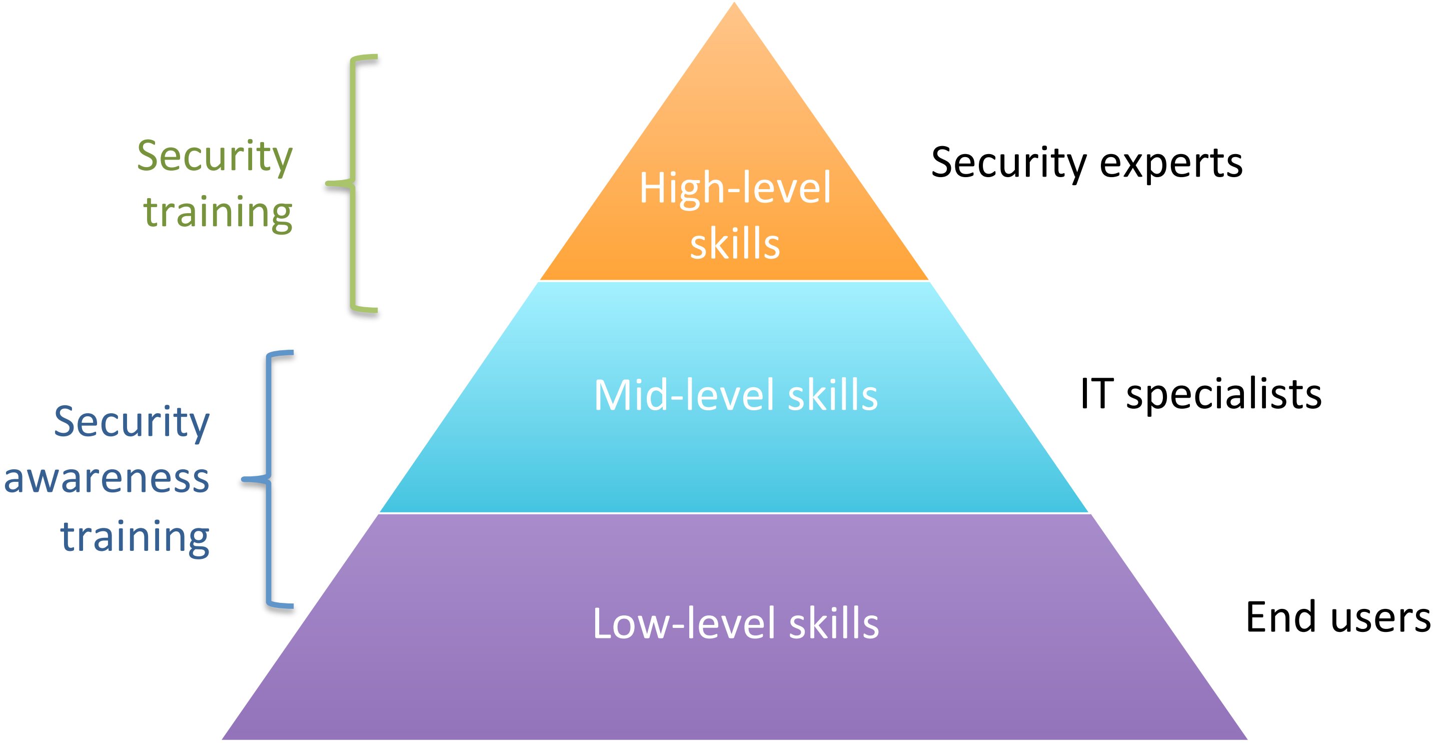
1. Motivation & overview
2. Making use of StarBED
3. Case studies
4. Summary

Motivation

- People have become more and more reliant on the Internet
  - A world in which devices and people are all connected together: the **Internet of Things** (IoT)
- Network communication makes life more convenient, but it also exposes users to cybersecurity risks, such as malware, phishing
  - It is necessary to conduct cybersecurity education and training as we perform at JAIST

Cyber range

- Environment for cybersecurity training
  - Facilitates learning and use of practical skills



Cyber Range Organization and Design

CROND

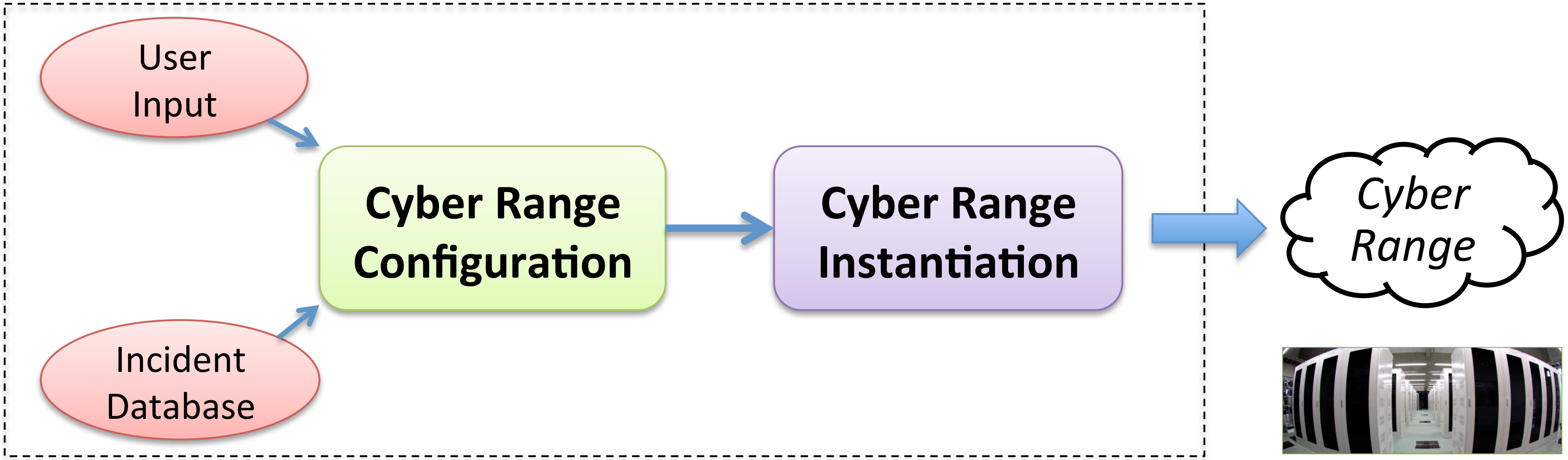
- NEC endowed chair at JAIST
  - 3 year period starting in FY 2015
- Two main directions
  - Cyber range architecture and design
    - Develop technologies and frameworks
  - Cybersecurity education programs and courses
    - Develop curriculum, training materials

Making use of StarBED

- Implementation and execution of cyber ranges, experiments, etc.

For IT & security professionals

- Use cyber ranges to acquire the practical skills for properly handling security incidents



User Input

Incident Database

Cyber Range Configuration

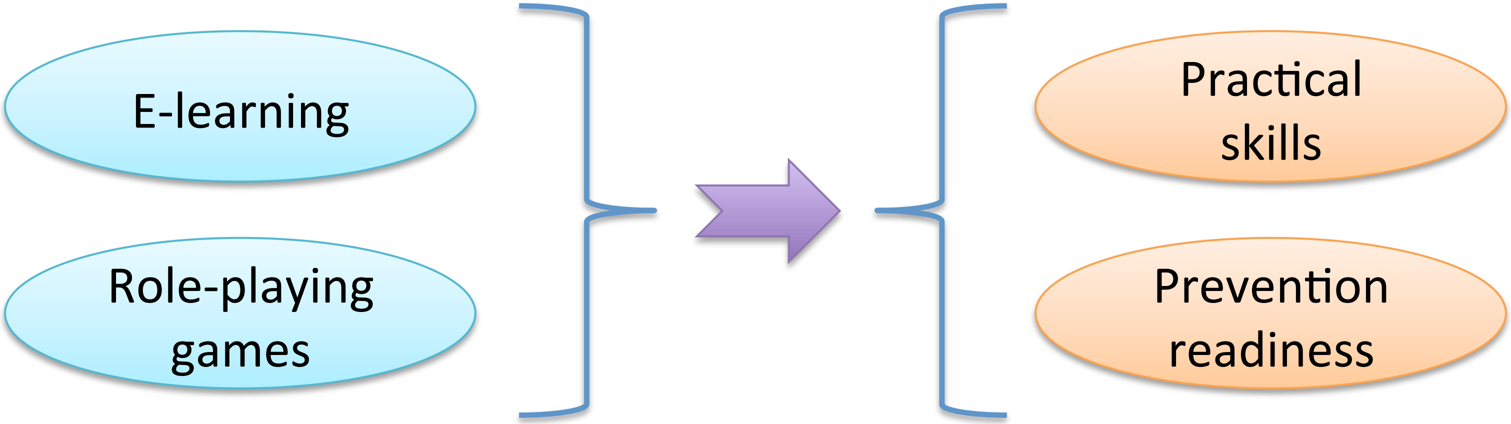
Cyber Range Instantiation

Cyber Range

Cyber Range Creation Framework

For regular computer users

- Use active education to gain awareness of potential cybersecurity risks



E-learning

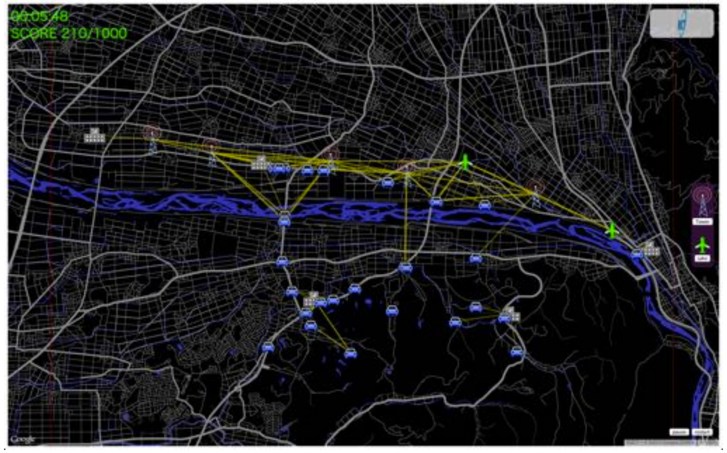
Role-playing games

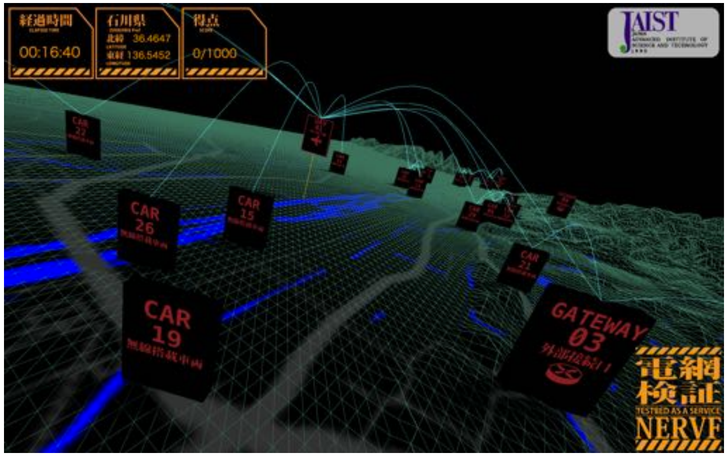
Practical skills

Prevention readiness

Network emulation

- Use network emulation to assess applications and protocols from the perspective of cybersecurity risks

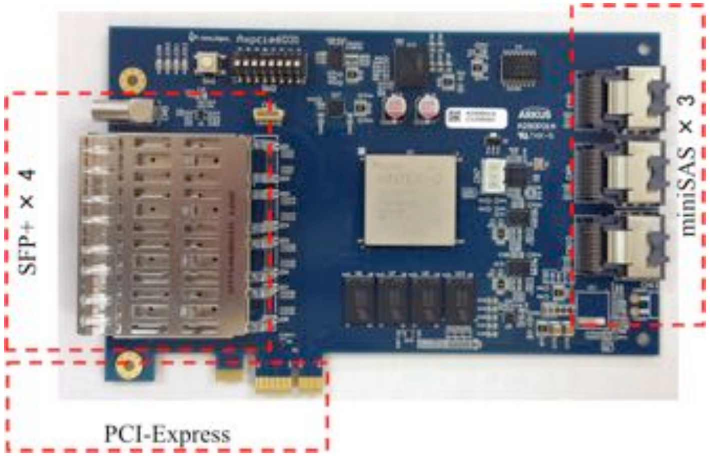


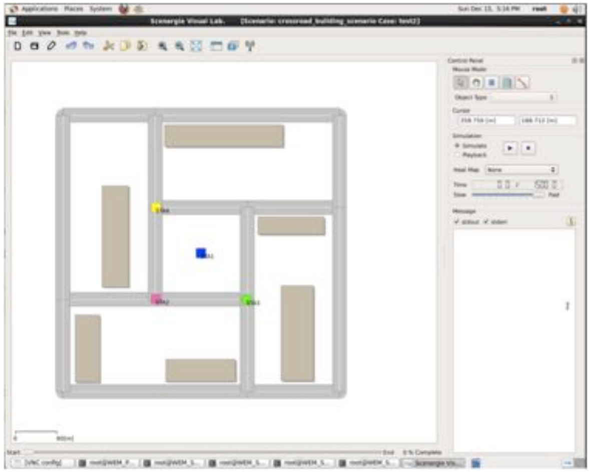


Network emulation framework: NERVF

IoT experiments

- Thorough experiments are required to make sure IoT technologies are operating safely





FPGA-based propagation emulator: StarWave
802.15.4 support (ongoing development)

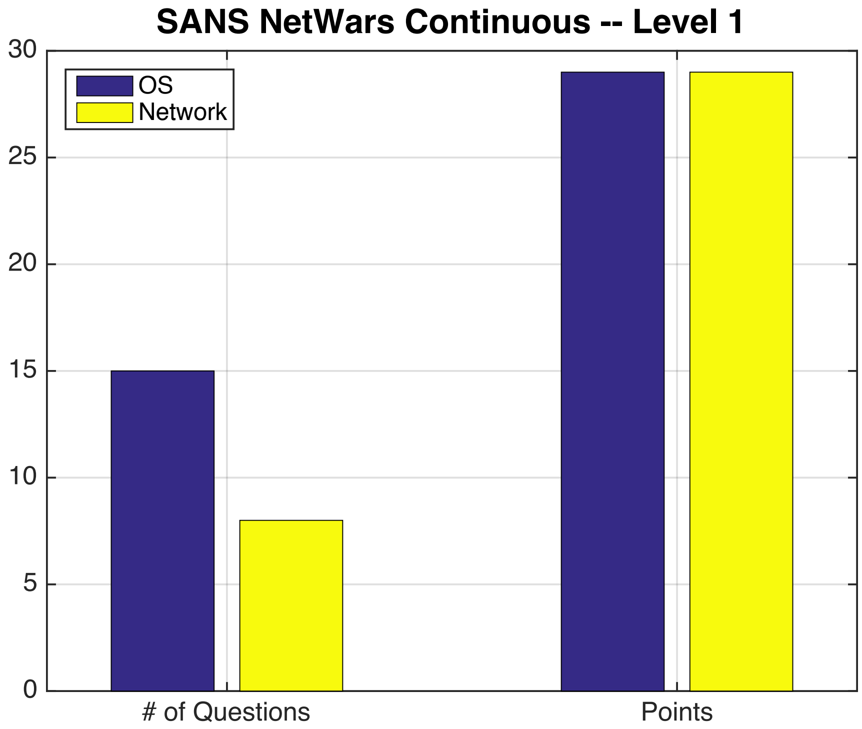
Case studies

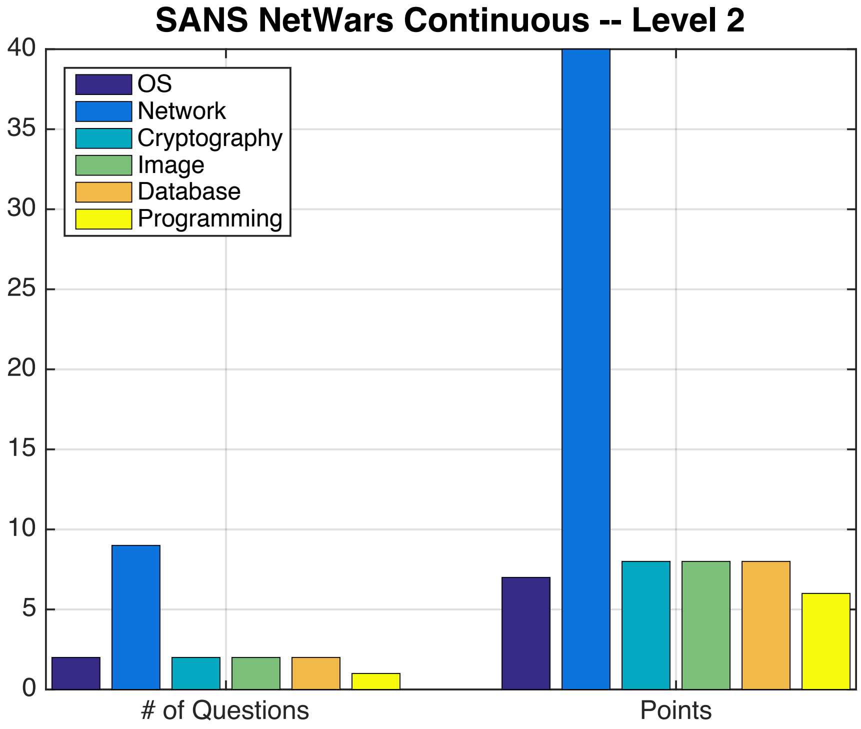
- SANS NetWars Continuous
  - Online training program of SANS Institute
  - 5 levels to be tackled during 4 months
  - Topics
    - Vulnerability Assessment
    - Packet Analysis
    - Penetration Testing
    - System Hardening
    - Malware Analysis
    - Digital Forensics and Incident Response

Levels 1 & 2: Summary

- **Level 1**
  - Analyze the configuration of a local machine to find security flaws
  - Evaluate browser forensic artifacts, command shell history, document metadata, and malware to discover crucial evidence
  - Analyze packets for evidence of attacks
  - Determine how an attacker pivoted through the network to gain access to a target machine
- **Level 2**
  - Analyze and isolate persistent, evasive malware
  - Analyze a system to determine and thwart attackers' techniques
  - Reconstruct network topologies and attack evidence from packet capture files
  - Crack local passwords and wireless crypto keys
  - Work with SQL databases to find security flaws and evidence

Levels 1 & 2: Break down



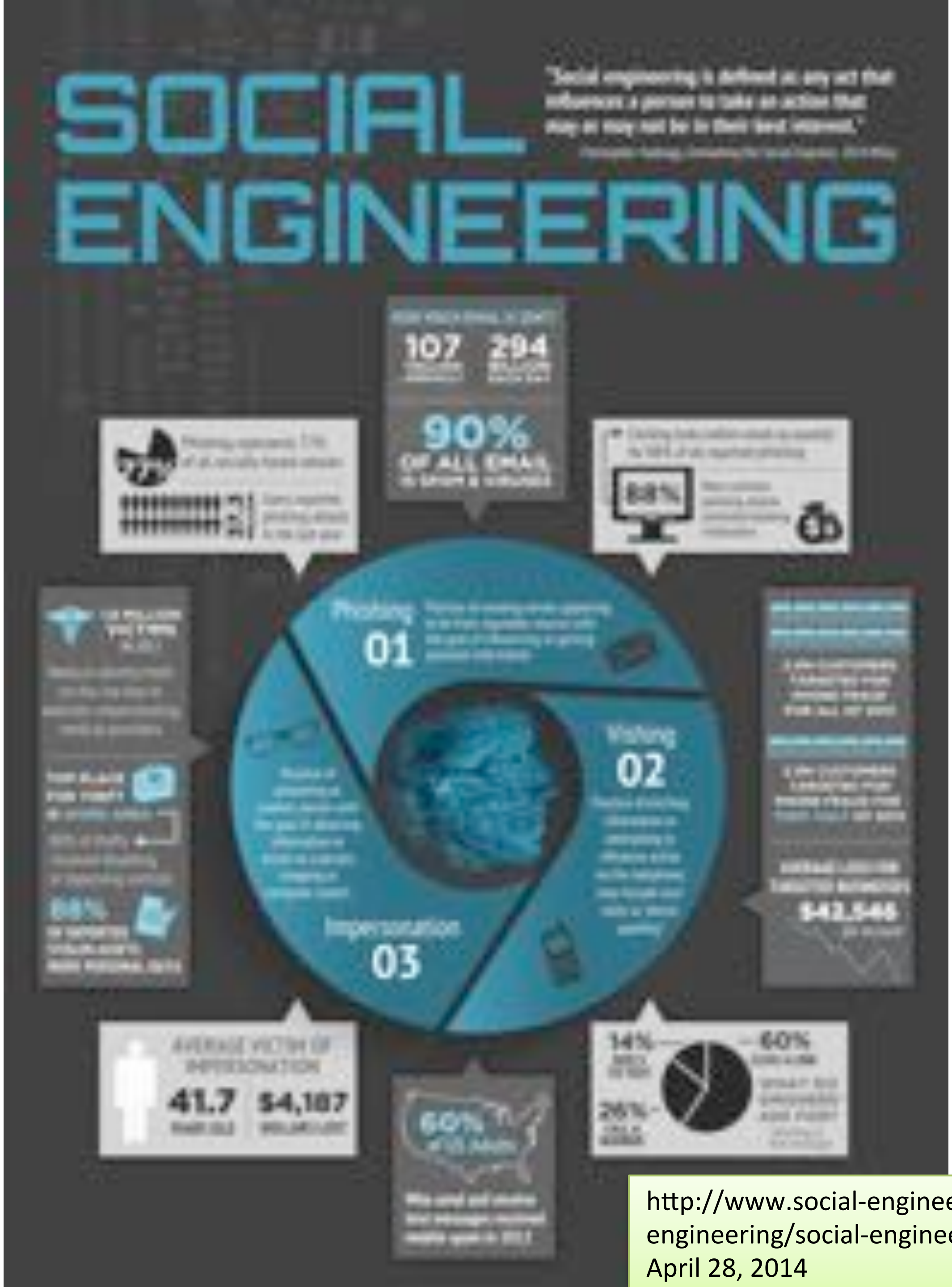


Total Questions: 23
Total Points: 58

Total Questions: 18
Total Points: 77

Security awareness training

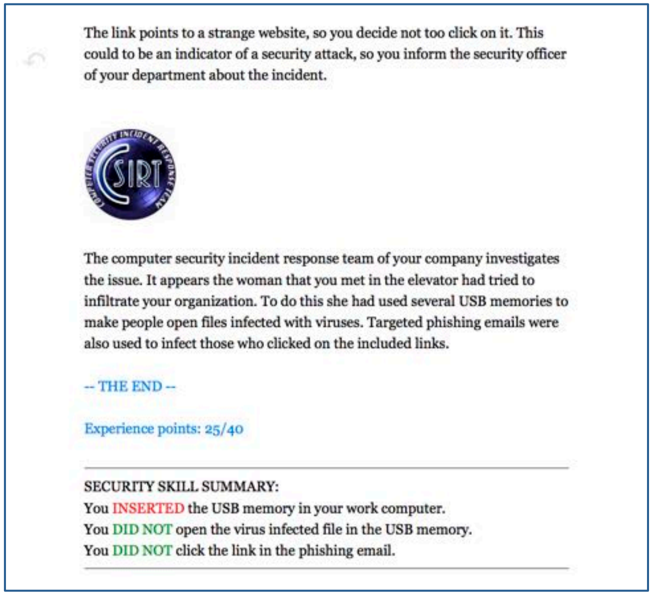
- Design security awareness training platform
  - Test basic security skills in a practical manner
  - Focus on social engineering attack prevention
- Use concept of gamification (serious games)
  - Engage users through emotions, competitive behavior, etc.
  - Incorporate social and reward aspects of games
  - Make education and training more effective


SOCIAL ENGINEERING
"Social engineering is defined as any act that influences a person to take an action that may or may not be in their best interest."
107
294
90%
OF ALL EMAIL
88%
Phishing
01
Vishing
02
Impersonation
03
$42,546
AVERAGE VICTIM OF IMPERSONATION
41.7
$4,187
60%
14%
60%
26%

http://www.social-engineer.org/social-engineering/social-engineering-infographic/
April 28, 2014

Game idea

- Example storyline (fragment)
  - Go to office
  - Meet person in elevator
  - He/she drops USB memory
  - Investigate USB memory



The link points to a strange website, so you decide not too click on it. This could to be an indicator of a security attack, so you inform the security officer of your department about the incident.

The computer security incident response team of your company investigates the issue. It appears the woman that you met in the elevator had tried to infiltrate your organization. To do this she had used several USB memories to make people open files infected with viruses. Targeted phishing emails were also used to infect those who clicked on the included links.

-- THE END --

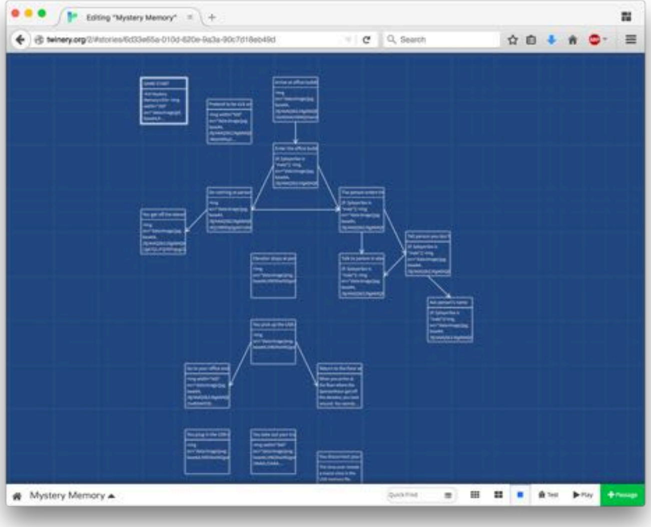
Experience points: 25/40

SECURITY SKILL SUMMARY:
You INSERTED the USB memory in your work computer.
You DID NOT open the virus infected file in the USB memory.
You DID NOT click the link in the phishing email.

- Tested skills
  - Pick up USB memory? Insert it in PC?
  - Open file on USB memory?
  - Click on link in email from person?

Implementation tool

- Twine: open-source tool for telling interactive, nonlinear stories (http://twinery.org/)
  - Stories can be extended with variables, conditional logic, images, CSS, and JavaScript
  - Publish directly to HTML
  - Stand-alone or browser interface
  - Used by RPG researchers for game prototyping



Summary

- We address the need for cybersecurity education and training through cyber ranges
  - Cyber Range Organization and Design (NEC endowed chair) @ JAIST
  - Architecture and design of cyber ranges
  - Education programs and courses
- StarBED is the infrastructure for the implementation and execution of cyber ranges
  - Already used by CYDER, SecCap and Hardening training programs
  - Also used for network emulation experiments

THANK YOU!

razvan@nict.go.jp